REMARKS/ARGUMENTS

No new matter is being added by virtue of the amendment to the claims.

Favorable action is respectfully requested.

Shown in the section below is a marked-up version of the changes made to the specification or claims by the current amendment. The section is captioned **"VERSION WITH MARKINGS TO SHOW CHANGES MADE"**.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In the claims:
Please amend the claims as shown below:

1. (Once Amended) A method of detecting states that are activated by a computer unit, in order to detect an unauthorized behavior or an unauthorized software program, the method comprising:

checking a set of values in a memory area of the computer unit or in a proprietary file ~~within~~ stored within the computer unit, with each set of values correspond to a state activated by the computer unit, wherein the checking includes calculating a maximum base count for entries in a defined registry segment; and

capturing each set of values to determine each state activated by the computer unit.

14. (Once Amended) An article of manufacture, comprising:

a machine-readable medium having stored thereon instructions to:

check a set of values in a memory area of the computer unit or in a proprietary file ~~within~~ stored within the computer unit, with each set of values correspond to a state activated by the computer unit, wherein the checking includes calculating a maximum base count for entries in a defined registry segment; and

capture each set of values to determine each state activated by the computer unit.

15. (Once Amended) An apparatus for detecting states that are activated by a computer unit, in order to detect an

unauthorized behavior or an unauthorized software program, the apparatus comprising:

means for checking a set of values in a memory area of the computer unit or in a proprietary file ~~within~~ stored within the computer unit, with each set of values correspond to a state activated by the computer unit, wherein the checking includes calculating a maximum base count for entries in a defined registry segment; and

communicatively coupled to the checking means, means for capturing each set of values to determine each state activated by the computer unit.

18. (Once Amended) A method of detecting states that are activated in an internal computer unit environment, in order to detect an unauthorized behavior or an unauthorized software program, the method comprising:

(a) monitoring an active window task manager for all identifiable window handles;

(b) intercepting operating system messages which are transmitted between a third-party application and an operating system;

(c) detecting change in a critical operating system file or third-party start-up file;

(d) detecting change in a critical aspect of a registry in the internal computer unit environment, including calculating a maximum base count for entries in a defined registry segment;

(e) sending an inner-process communications message to any identifiable window handle which resides within the active task manager;

(f) sending a real time forensic report to a monitor station, the real time forensic report defining the state of the detection.

19. (Once Amended) A method of processing computer registry information, in order to detect an unauthorized behavior or an unauthorized software program, comprising:

storing all computer registry information in memory; and

recording the computer registry information into a structure file for transmission, to permit detection an unauthorized behavior or an unauthorized software program.

20. (Once Amended) A method of checking all computer registry information in a real-time computer environment, the method comprising:

comparing the current computer unit machine registry activity state to the previously recorded registry state to detect unauthorized changes to a registry of the computer unit, including calculating a maximum base count for entries in a defined registry segment.

21. (Once Amended) A method of storing electronically mapped directories and files, comprising:

providing electronically mapped directories which are required for the start-up of third-party applications installed within a computer unit; ~~and~~

mapping the directories into a structured file;

calculating a maximum base count for entries in a defined registry segment.

22. (Once Amended) A method of checking computer start-up directories and files, comprising:

comparing the current computer unit machine directory and file activity state to the previously recorded directory and file state to detect unauthorized changes to start-up

directory and files of a computer unit, including calculating a maximum base count for entries in a defined registry segment.

23. (Once Amended) A method of monitoring operating system (O/S) messages, comprising:

comparing messages to an authorized activity listing file to detect unauthorized activity, including calculating a maximum base count for entries in a defined registry segment.

24. (Once Amended) A method of reporting the unauthorized internal activity in the computer unit, comprising:

detecting the unauthorized activity; and

transmitting a report of the activity to a second computer unit and calculating of a maximum base count for entries in a defined registry segment.

25. (Once Amended) A method of detecting unauthorized activity in a computer unit, comprising:

reporting an active focus window handle, in a real-time environment, ~~by comparing the~~ by comparing the messages to an authorized activity listing file, to detect unauthorized activity, including calculating a maximum base count for entries in a defined registry segment.

26. (Once Amended) An apparatus for detecting states that are activated by a computer unit, the apparatus comprising:

a first engine capable to checking a set of values in a memory area of the computer unit or in a proprietary file ~~within~~ stored within the computer unit, with each set of values correspond to a state activated by the computer unit; and

communicatively coupled to the first engine, a second engine capable to capture each set of values to determine each state activated by the computer unit and to calculate a maximum base count for entries in a defined registry segment.

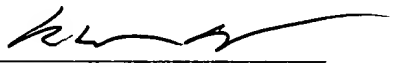
CONTACT INFORMATION

If the Examiner has any questions or needs any additional information, the Examiner is invited to telephone the undersigned attorney at (805)681-5078.

Also enclosed herewith is a copy of a previously-filed Change Of Correspondence Address for the above-referenced application, filed by the undersigned attorney of record on 13 January 2003. The undersigned attorney of record respectfully requests that the correspondence address for the above-referenced application is updated.

Date: February 25, 2003

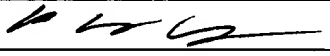
Respectfully submitted,
Robert F. Terry



By: Arnold M. de Guzman
Attorney for Applicant
Reg. No. 39,955
805.681.5078
805.681.5076 (fax)

Please send correspondence to:

Arnold M. de Guzman
DeGuzman & Carpenter LLP
5276 Hollister Avenue, Suite 160
Santa Barbara, CA 93111

CERTIFICATE OF MAILING			
I hereby certify that this correspondence, including the enclosures identified herein, is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Washington, D.C. 20231 on the date shown below. If the Express Mail Mailing Number is filled in below, then this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 C.F.R. 1.10.			
Signature:			
Typed or Printed Name:	Arnold M. de Guzman, Reg. No. 39,955	Dated:	**Feb. 25, 2003**
Express Mail Mailing Number (*optional*):	**EU181981533US**		